

COALITION FOR ONLINE ACCOUNTABILITY

WWW.ONLINEACCOUNTABILITY.NET

C/O MITCHELL SILBERBERG & KNUPP LLP • 1818 N STREET N.W., 8TH FLOOR • WASHINGTON, D.C. 20036-2406
TEL: (202) 355-7906 • FAX: (202) 355-7899 • E-MAIL: INFO@ONLINEACCOUNTABILITY.NET

Before the United States Department of Commerce
National Telecommunications and Information Administration
International Trade Administration,
National Institute of Standards and Technology

Response of the Coalition for Online Accountability

to Notice of Inquiry on

Information Privacy and Innovation in the Internet Economy
(75 Fed. Reg. 21226, Apr. 23, 2010)

[Docket No. 100402174-0175-01]

Submitted by
Steven J. Metalitz
Mitchell Silberberg & Knupp LLP

Counsel to Coalition for Online Accountability

June 14, 2010

American Society of Composers
Authors & Publishers (ASCAP)

Entertainment Software Association (ESA)

Software & Information Industry Association (SIIA)

Broadcast Music Inc. (BMI)

Motion Picture Association of America (MPAA)

Time Warner Inc.

Recording Industry Association of America (RIAA)

The Walt Disney Company

Counsel: Steven J. Metalitz (met@msk.com)

The Coalition for Online Accountability (COA) appreciates this opportunity to respond to the Notice of Inquiry on Information Privacy and Innovation in the Internet Economy (“NOI”). 75 Fed. Reg. 21226 (Apr. 23, 2010).

About COA

COA consists of eight leading copyright industry companies, trade associations and member organizations of copyright owners, all of them deeply engaged in the use of the Internet to disseminate creative works. These are the American Society of Composers, Authors and Publishers (ASCAP); Broadcast Music, Inc. (BMI); the Entertainment Software Association (ESA); the Motion Picture Association of America (MPAA); the Recording Industry Association of America (RIAA); the Software and Information Industry Association (SIIA); Time Warner Inc.; and the Walt Disney Company. The Coalition’s main goal since its founding a decade ago (as the Copyright Coalition on Domain Names) has been to preserve and enhance online transparency and accountability. A predominant focus has been to ensure that data concerning domain name registrations and IP address allocations remain publicly accessible, accurate and reliable, as key tools against online infringement of copyright. This data is also essential in combating trademark infringement, cybersquatting, phishing, and other fraudulent acts online.

Introduction

The focus of the NOI appears to be on (1) businesses that collect information from or about individual consumers in the course of engaging in e-commerce activities, and (2) the individuals themselves, whose data could be manipulated or abused by those collecting businesses. The perspective of COA participants is somewhat different: the protection of the legal rights of creators and distributors of copyrighted material in the e-commerce environment. Not surprisingly, this perspective does not correspond directly to the topic areas specifically identified in the NOI. Our perspective is, however, directly responsive to the question posed by the NOI: “whether current privacy frameworks, or frameworks that are in development, create barriers to innovation on the Internet.” NOI at 21228.

COA and its members fully support the NOI’s goal, “to identify policies that will enhance the clarity, transparency, scalability and flexibility needed to foster innovation in the information economy.” Id. at 21227. The online environment offers exciting opportunities for new ways to create, deliver and disseminate creative works. Through this medium, works such as musical compositions, recordings, movies, and videogames are reaching ever wider audiences through ever more diverse distribution and performance channels. We believe that developing and safeguarding a thriving online marketplace for such works is a key element of the innovation that a healthy information economy requires.

Widespread infringement of copyright has been a pervasive feature of the online environment in recent years. This represents a clear threat to a healthy information economy and to the innovation that underpins it. The substantial investments in innovation that copyright owners undertake in order to develop a legitimate online marketplace in their works cannot be sustained without adequate protections against copyright theft. We appreciate the consistent and strong support voiced by the leadership of the Department of Commerce and its constituent

agencies for the central role of intellectual property enforcement in promoting innovation in the Internet economy. See, e.g., remarks of Under Secretary Kappos before Center for American Progress (June 2, 2010) at http://www.uspto.gov/news/speeches/2010/Kappos_CAP_speech.jsp (“strong intellectual property protection and its effective enforcement will fuel innovation and jump-start our economy”); remarks of Assistant Secretary Strickling before the Media Institute (Feb. 24, 2010) at http://www.ntia.doc.gov/presentations/2010/MediaInstitute_02242010.html (enumerating as a key challenge “How do we protect against illegal piracy of copyrighted works and intellectual property on the Internet while preserving the rights of users to access lawful content?”).

COA participants are strongly committed to the goal of clear and enforceable privacy protections in the online environment. Without such protections, the necessary public confidence in the information economy can be jeopardized. But widespread disrespect for intellectual property rights online could have the same deleterious effects. If the online marketplace comes to resemble a thieves’ bazaar, both legitimate merchants and prudent customers will be reluctant to enter it.

All COA participants, like others in the copyright sector, actively engage in efforts to detect and to prevent online copyright theft, and have invested heavily in programs to do so. These efforts depend upon our continued ability to access and process publicly available information concerning illegal online activities, and to share this information as appropriate with other key stakeholders in the Internet environment, including Internet service providers, e-commerce marketplaces, and law enforcement agencies. Maintaining access to this information, and taking steps to ensure that it is accurate, reliable, and current, will not threaten the privacy interests of consumers. Rather, it will enhance their online experience and encourage greater participation in the information economy.

In this submission, COA wishes to emphasize that privacy policies must be carefully calibrated to minimize adverse impacts on legitimate activities carried out to protect copyright and other intellectual property rights online, through the use of this publicly available data. We are confident that this calibration is fully consistent with robust privacy protections for the personal information of consumers and their legitimate online activities. We urge NTIA and the other DOC agencies participating in the Task Force to keep in mind the need for such calibration, both in the context of developing improved privacy policies under U.S. law, and in engaging with our trading partners on these issues.

Two brief examples of the needed calibration can be provided. The first involves data on registrants of domain names, while the second concerns Internet Protocol addresses.

Domain Name Whois

Domain name registration information has been publicly accessible through a service labeled Whois since the earliest days of the domain name system, even predating the World Wide Web. Public access to Whois data is essential to the investigation and prompt resolution of instances of copyright piracy and trademark counterfeiting online. The investigation of virtually every such case involves the use of Whois data. For example, when an investigator seeks to

determine who is responsible for a website where infringing activity is taking place, a review of the Whois data for the domain name which resolves to that site is usually the first step. Once the responsible party has been identified, the copyright owner or its agent is in a position to request that the party obtain a license or cease the infringing activity, or, where appropriate, to begin enforcement action.

But Whois data's valuable uses are by no means limited to the sphere of intellectual property protection. Access to Whois data is critical to dealing with instances of phishing, distribution of malware, network attacks, and online frauds of all kinds. This data is essential to law enforcement, of course, but also to private parties such as copyright and trademark owners, whose independent enforcement of their rights allows law enforcement to conserve scarce resources. Indeed, virtually every Internet user benefits from public accessible Whois. Whois provides greater transparency, so that end users know more about the parties with whom they – or their children – are interacting online. This is a fundamental prerequisite to building public confidence in the information economy.

For these reasons, COA urges the Commerce Department to maintain and redouble its long-standing efforts to preserve public access to Whois data, and to improve its quality, reliability, and timeliness. The locus for such efforts includes, though it is by no means limited to, the Internet Corporation for Assigned Names and Numbers (ICANN), where binding policy on these issues for the generic Top Level Domains is hammered out, and where continued U.S. leadership within the ICANN Governmental Advisory Committee is especially critical.

While many other national governments share this perspective on the importance of maintaining public access to Whois, some commentators insist that the long-standing system of publicly accessible Whois is incompatible with the privacy laws of some countries. It is claimed that these laws require restrictions on what data about domain name registrants is made available through Whois, and/or that these laws demand that public access to Whois be wholly or substantially suppressed. Such an expansive interpretation of privacy laws threatens to cloud the transparency needed for a sound information economy. As such issues arise, we urge the Commerce Department to engage with our trading partners to ensure that the implementation of their national privacy laws accommodates continued unfettered access to Whois data for the valuable purposes summarized above.

IP Address Information

The label "Whois" also refers to information about the allocation of blocks of Internet Protocol (IP) addresses, which are the numeric addresses for all resources connected to the Internet. Access to this information is extremely important for enforcement against copyright piracy, trademark infringement, and other forms of misconduct carried out online. When such misconduct is associated with a particular IP address, Whois enables the investigator to identify the Internet service provider or other entity to which the IP address was initially assigned, and also to learn of sub-allocations to other providers, though rarely, if ever, to the end-user. Accessibility and reliability of IP address Whois data, including ensuring that all sub-allocations are entered into the database and kept up to date, are also critical issues for attention from the U.S. government.

Since IP address information travels routinely and visibly with many communications over the Internet, and since even the Whois information associated with such addresses generally cannot, by itself, identify any end-user, public access to and use of such data should have little if any impact on privacy or free expression concerns. However, under expansive interpretations of their national privacy laws, government agencies and courts in some countries have erected obstacles to the collection and use of IP address information in private sector efforts to enforce copyright in the online environment.¹

These interpretations are particularly problematic to the extent that they impede cooperative efforts of right holders, ISPs and other information economy stakeholders against copyright theft. For instance, when an investigator acting on behalf of a copyright owner observes high-volume copyright infringements by a user of an illicit peer-to-peer (p2p) service, questions have been raised under some national privacy laws about the collection of the user's IP address by the investigator; the furnishing of that address to the ISP to which the address has been allocated; and the linking of that address by the ISP to a particular subscriber, for the purpose of forwarding a warning notice regarding the infringing activity. In this example, expansive interpretations of privacy laws clearly disserve the goal of promoting innovation in the information economy. Such a privacy law framework could make it virtually impossible for responsible parties to work together to address illegal activity that, left unchecked, could easily inundate the legitimate online marketplace in copyrighted works.

To a considerable extent, the impediments to collecting and using IP address data in online copyright enforcement efforts flow from the classification of such information as "personal data," the collection or processing of which is extensively regulated under the privacy laws of a number of countries. Legislation to regulate collection and use of IP addresses as "personally identifiable data" under US law has also been proposed. See, e.g., Staff Discussion Draft of House legislation "to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual," May 3, 2010, available at http://www.boucher.house.gov/images/stories/Privacy_Draft_5-10.pdf. Such proposals risk erecting unintended obstacles to the robust enforcement of copyright that is essential to promoting innovation in the Internet economy. COA urges the Department of Commerce to engage actively on these issues, both in the development of U.S. privacy law and policy, and in consultations with our trading partners, to ensure that that the "personal data" rubric is not counterproductively extended to impede responsible use of IP address data to detect and deal with instances of online copyright infringement.

¹ See, for example, the legal analyses of the situation in several European Union member states in the reports found at http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf and http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_en.pdf. But see *EMI Records v. Eircom Ltd.*, [2010] IEHC 108 (Republic of Ireland High Court, Apr. 16, 2010), available at <http://www.bailii.org/ie/cases/IEHC/2010/H108.html>, finding such uses fully compatible with Irish data protection law. See also *Arista Records LLC v. Doe 3*, No. 09-0905, (2d. Cir., April 29, 2010), slip op. at 16 ("to the extent that [online] anonymity is used to mask copyright infringement or to facilitate such infringement by other persons, it is unprotected by the First Amendment.").

Conclusion

COA appreciates your consideration of our views and would be glad to respond to any questions concerning this submission.

Respectfully submitted,

Steven J. Metalitz, counsel to COA
Mitchell Silberberg & Knupp LLP
1818 N Street, NW, 8th Floor
Washington, DC 20036 USA
Tel: +1 (202) 355-7902
Fax: +1 (202) 355-7899
E-mail: met@msk.com